

STATEMENT OF  
SCOTT CHARBO  
CHIEF INFORMATION OFFICER  
U.S. DEPARTMENT OF AGRICULTURE  
BEFORE THE  
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,  
INTERGOVERNMENTAL RELATIONS AND THE CENSUS  
COMMITTEE ON GOVERNMENT REFORM  
U.S. HOUSE OF REPRESENTATIVES

June 24, 2003

Mr. Chairman and Members of the Subcommittee, thank you for inviting me here today to discuss the challenges and opportunities we face and the progress we are making on protecting the information and systems entrusted by the public to the U.S. Department of Agriculture (USDA). With your permission, I will submit my testimony for the record.

At USDA, I am responsible for computer systems that support billions of dollars in annual program benefits. Information stored on these systems includes: Federal payroll data, market sensitive (crops, farm, commodities, statistical) data, geographical data, information on food stamps and food safety, and proprietary research data. This information is one of USDA's greatest assets. Threats to these assets are numerous, ranging from outright transferring of funds and personal/customer/program information -- to cyber-attacks that leave our information systems crippled or inoperable. Audit reports conducted by both USDA's Office of Inspector General (OIG) and the General Accounting Office (GAO), as well as our own review, have identified significant weaknesses in our overall computer security program.

Mr. Chairman, as you know, our push to deliver more and more services electronically makes protecting these services a high priority. I believe we at USDA are improving in the job we do in this area. Currently, we are implementing significant changes in how we manage information and IT security positions at USDA. However, our size, decentralized organization, and the wide array of hardware and software in use, combined with the magnitude of today's cyber threats, mean that we have a tremendous amount of work remaining to reduce the risk to our information assets to an acceptable level.

#### The State of Information Security at USDA

USDA's 18 agencies and 12 staff offices together employ over 100,000 people. The Department's fiscal year (FY) 2004 Budget requests about \$2.25 billion for IT investments to support the services and products we deliver. Historically, each agency/office funded and managed its own IT investments independent of all other organizations in the Department. Likewise, security controls employed to protect these investments have been selected independently. This decentralized management structure has created an environment where some USDA agencies have addressed the issues of security and risk, while many others have not.

Today, ensuring a high level of information and computer security in every USDA agency is a critical issue for USDA's management. Representative of this commitment, we have begun holding our senior executives accountable by including a performance measure in their annual performance plan related to the security of their information and systems. With funds from Congress, we are continuing to build a central cyber security

program that is providing our agencies with uniform policies, guidance, tools, and program management; we are setting clear cyber security goals and then assisting agencies in meeting them. Through our IT capital planning and investment control process, we are also doing a better job integrating security into all phases of our IT projects lifecycle, from initial planning to system retirement.

This story of good progress and change with much more work to do is represented in our numbers:

- In FY 2004, USDA plans to spend about \$68 million to protect our information assets. This represents an increase of 6% over the \$64 million in cyber security spending estimated for FY 2003.
- In the past year, 6 agencies completed risk assessments of their cyber security programs from qualified security contractors, with an additional 4 now underway. Similarly, 9 USDA organizations completed independent security risk assessments on 26 separate systems. Many others are currently in the process of completing assessment of their respective programs and systems.
- In the Office of Management and Budget's review of the 51 systems in our FY 2004 Major IT Systems Portfolio, 43% (or 22 systems) received a passing security score. This is the first year we received security scores from OMB.

With the additional planning and training we are conducting this year, I expect all USDA's FY 2004 investments to receive passing scores from OMB.

- Over the past two years, we have deployed intrusion detection and anti-virus software across the Department. Just this month, we held a training session for agency IT staff on how to deploy the Department's latest patch-management software solution. By deploying patch management software we will be able to ensure the most recent releases of software patches are consistently and timely installed across our enterprise.
- Finally, our USDA Government Information Security Reform Act (GISRA) Plan of Actions & Milestones (POA&M) currently shows that we are taking 1,405 distinct actions to address 243 program and system level weaknesses. While the numbers we report will go up or down as the threats to our systems change, I am confident we will see progress in our POA&M reporting.

At USDA, we are fortunate to have a strong information security officer and staff, who drive our information and IT security efforts. They have been instrumental in building our program over the past three years, and deserves much of the credit for the accomplishments and activities I am talking about here today.

USDA Actions to Correct Deficiencies Reported in FISMA and Financial Reporting

Mr. Chairman, in your invitation to this hearing, you asked me to discuss the actions that we are taking to remedy the deficiencies reported in both our GISRA and financial reporting. While USDA's cyber security program covers the full range of technical and management disciplines, I will focus my comments on our highest priority related initiatives.

- Security Awareness: Information Assurance starts with employee education. All employees, from general users to system administrators to senior executives, need to understand the threats to the assets they manage and their cyber security responsibilities. We are spreading the word across USDA through online courses like the government standard GoLearn.gov E-Learning program, classroom training, as well as numerous technical and management forums.

Recognizing the importance of this issue, the Secretary and I are personally raising this issue at our Subcabinet meetings and during regular briefings for our Agency Heads.

- Disaster Recovery and Business Resumption Planning: We are making good progress establishing executable Business Resumption and Disaster Recovery Plans for USDA's most critical information systems. With funding from Congress, we are providing the methods, policy, training, tools, guidance and oversight to agency program and technical managers. By the end of this calendar

year, I expect to see high-quality, consistent, and verified Disaster Recovery and Business Resumption plans for our highest priority systems.

- Certification & Accreditation: The Office of Management and Budget has made it clear that our information systems must be fully certified and accredited. At USDA, we are finalizing a standard methodology and process for our agencies to use to verify and attest that information system security: 1) functions as required, and 2) assures the confidentiality, availability, and integrity of its data and processes. Certification is an intensive, time consuming, and costly process. With this in mind, our goal is to certify & accredit all of our highest priority systems by July 2004.
- Integrating Security into the IT Capital Planning and Investment Control Process: As I mentioned earlier, we revised our IT Capital Planning and Investment Control guidance to ensure system owners address security in all stages of an IT project's lifecycle. In our IT plans, investment owners must demonstrate how they are preparing to secure investments, and provide specific milestones for achieving critical security elements. This year, we are also strengthening our training for agency IT planners to ensure they understand the security and privacy requirements for their IT investments.

USDA Procedures, Processes and Structures to Institutionalize Daily Management of Information Security Risks

Mr. Chairman, you also asked me to discuss the procedures, processes and structures we are putting in place to assist in the transition from once-a-year reporting to institutionalization and daily management of information security risks.

At USDA, the Federal Information Security Management Act of 2002 (FISMA) reporting process has helped us more clearly track specific cyber security weaknesses, which in turn is helping us make better decisions, while holding us more accountable for results.

Currently, our agencies along with my office update all identified information security weaknesses and related corrective actions in a central FISMA POA&M database on a quarterly basis. We use this information in our quarterly and annual reports to OMB. We also use this information as a management tool, verifying and validating agency plans, and analyzing this information in the context of our knowledge of agency progress. When we began this process, there was some uncertainty as to the quality and comprehensiveness of our data. However, as our process matures, we have seen a significant improvement in the quality of information reported. This is moving USDA's security posture from reactive to proactive.

Our goal must be to continue integrating information security planning and reporting into our day-to-day IT management process. The Department's Enterprise Architecture (EA) and IT Portfolio Management initiatives will help us do this. Applying OMB's Federal Enterprise Architecture guidance, we have begun documenting the EA layers (business processes, data, applications, and technology infrastructure). Analyzing and tracking this

information, across all USDA agencies and offices, will enable us to better leverage our information and IT resources. Integrating our security architecture into each layer of the EA will help us ensure we're providing the right level of security for our data, applications, and technology. Similarly, our IT Portfolio Management initiative will allow us to consistently track the achievement of project milestones, including security milestones, for our IT investments.

Finally, I want to mention one modernization project that is critical to strengthening cyber security at USDA. We are redesigning our long distance telecommunications network to support the growing demand for E-Government services. Currently, the mostly decentralized structure of USDA's interconnected data centers and telecommunications networks means that the Department is only as strong as its weakest links. Once implemented, our future Universal Telecommunications Network will greatly improve our ability to verify the integrity and confidentiality of data transmitted over the network.

Mr. Chairman, thank you again for the opportunity to be here today. I am proud of the progress we are making in this area, and look forward to answering any questions you may have.